IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

STEVEN BOWERS,

Plaintiff,

v.

OPINION and ORDER

COUNTY OF TAYLOR, BRUCE DANIELS, and MELISSA SEAVERS,

20-cv-928-jdp

Defendants.

This case arises from a government agency's search of an online account created by one of its employees. It poses close questions of Fourth Amendment law concerning online accounts and the rights of public employees.

Plaintiff Steven Bowers was a sergeant for the Taylor County sheriff's department. In 2017, the department started working with a television show called *Cold Justice*, a true-crime series that investigates unsolved crimes. The department gave the crew members access to one case file, but Bowers began sharing other case files with them, even though he didn't have permission to do so. After Bowers admitted what he had done, Sheriff Bruce Daniels directed IT director Melissa Lind (formerly Melissa Seavers) to try to access Bowers' Dropbox account, where Daniels believed that Bowers had stored the files. Lind was able to do so because the Dropbox account was linked to Bowers's work email. Lind changed Bowers's account password, accessed the account, and found the case files.

Bowers contends that Daniels and Lind violated the Fourth Amendment by failing to obtain a warrant before changing his password and accessing his account. He claims damages for "mental suffering, anguish, fear, humiliation, loss of personal freedom, and expenses."

Dkt. 10, ¶ 36. Defendants move for summary judgment, contending that the search was lawful and, even if not, they are entitled to qualified immunity. Dkt. 28.

The general rule is that a warrant is required for searches of private property. But there are more lenient standards involving some searches conducted by government employers. The Dropbox account was Bowers's personal account, and it wasn't stored on county servers, factors tending to support Bowers's contention that a warrant was required. But other factors point the other way, including that Bowers linked the account to his work email and he placed work files taken from a work computer into the account. The account was password protected, but Bowers had shared access with several others.

In the court's view, defendants' search was distinct from a typical workplace search, and the Dropbox account was sufficiently private to fall within the general warrant requirement. But the court reaches that conclusion only by extending principles from current precedent and following the reasoning of courts from other circuits. Bowers hasn't cited analogous cases from the Supreme Court or the Court of Appeals for the Seventh Circuit, and the more general case law he cites doesn't apply with obvious clarity to his situation. Under these circumstances, defendants did not violate any clearly established rights, and thus they are entitled to qualified immunity. The court will grant their motion for summary judgment.

BACKGROUND

The following facts are undisputed except where noted.

In January 2017, Taylor County entered a contract with the producers of *Cold Justice*, a reality television show that featured a former prosecutor and former investigators who attempted to solve "cold cases." In accordance with the agreement, the county gave the

producers access to files about what the parties call "the Monte case," involving an unsolved murder in Taylor County.

Bowers was a sergeant for the Taylor County sheriff's department at the time. He began speaking with staff on the tv show about other cold cases. The parties refer to one of those cases as the "V murder case."

Without obtaining permission or notifying anyone at the sheriff's office, Bowers took electronic files from the V murder case and copied them to his account with Dropbox, a cloud-based storage website. Bowers provided two versions of how he accomplished this.[1] But it's undisputed that he originally took the files from a county computer.

Bowers had created the Dropbox account using his work email address in 2014, but Dropbox isn't affiliated with the county. He used his work email address and a password that he created to log in to the account. He also used his own funds to pay for the account. He stored both personal and work-related files on the account.

Again without authorization, Bowers gave two of the show's employees and his girlfriend access to the Dropbox account, which allowed them to view the V murder case files. He did not share his password with them.

In late February 2017, Chief Deputy Larry Woebbeking overheard crew members from the show talking about Taylor County cases other than the Monte case and about reading case

[1] During an investigatory interview conducted in June 2017, which was under oath, Bowers testified that he opened the internet browser on a county computer, went to the Dropbox website, and dragged the electronic files from the county's server to a folder in his Dropbox account. Dkt. 37-6, at 75:25–76:11 and 105:19–106:14. In an answer to an interrogatory, Bowers stated that he "uploaded the case files from an electronic storage device to his Dropbox at home through his personal computer." Dkt. 31-1, at 5. This discrepancy has no bearing on the outcome of the case, so the court need not decide which version is correct..

files in their hotel room. Around the same time, he overheard crew members talking about receiving documents on Dropbox. Woebbeking suspected that Bowers had given the crew members confidential information and documents about other cases because no department employee other than Woebbeking and Bowers had been working with the show that day. Woebbeking told Sheriff Daniels about his suspicion.

A couple of days later, the department data records manager told Daniels that Bowers had instructed her to retrieve some case files and share them with one of the show's producers. The records manager also said that she believed files related to the V murder case were on Dropbox. Daniels confronted Bowers, who admitted that he had shared case files, including the V murder case file, with show producers. Bowers later returned paper copies of files that he had given to the show employees.

After speaking with the district attorney, Bowers asked IT Director Lind to access Bowers's county email account and the Dropbox account to look for information related to the V murder case. Lind accomplished this by: (1) going to the Dropbox website and entering Bowers's work email address to use Dropbox's "lost password" feature; (2) signing into Bowers's work email account and changing his Dropbox password; and (3) using the new password to sign in to the Dropbox account. Once she gained access to the account, Lind discovered a folder associated with the V murder case. She opened the folder, which contained many confidential case records.

Bowers has been charged with misconduct in public office, in violation of Wis. Stat. § 946.12(2). He is on administrative leave pending resolution of the criminal proceedings.[2]

[2] Neither side contends that the criminal proceedings in state court have any bearing on this case, so the court need not consider whether any claims or issues are precluded by those proceedings. *See Polzin v. Gage*, 636 F.3d 834, 838 (7th Cir. 2011) (bar on civil cases that

The court will discuss additional facts as they become relevant to the analysis.

ANALYSIS

A. Overview of the claims and issues

The Fourth Amendment to the United States Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Bowers's primary claim is that defendants violated his rights under the Fourth Amendment by unreasonably searching his Dropbox account. He doesn't contend that defendants violated the Fourth Amendment by searching his work email.

Bowers also contends that defendants unreasonably "seized" his account password by changing it without his permission. As defendants point out, Bowers didn't raise that seizure claim in his complaint. Rather, Bowers originally contended that defendants seized his account by "locking [him] out" out of the account. Dkt. 10, ¶ 38. Bowers has abandoned the lockout claim and replaced it with a new one. But it is well established that a plaintiff may not amend his complaint through his summary judgment opposition brief. *See Anderson v. Donahoe*, 699 F.3d 989, 997 (7th Cir. 2012). In any event, even if Bowers had included the seizure claim in his complaint and even assuming that a password is an "effect" and that changing a password is a "seizure" within the meaning of the Fourth Amendment, changing Bowers's password was simply a precursor to the search of his account. And Bowers identifies no reason why the search would be valid, but the "seizure" wouldn't be. So the court will focus on the search.

---

undermine criminal conviction can be waived); *Klingman v. Levinson*, 114 F.3d 620, 627 (7th Cir. 1997) (issue preclusion can be waived).

The first substantive question in this case is whether Bowers had a reasonable expectation of privacy in his Dropbox account. If he didn't, his Fourth Amendment claim fails. If he did, the next question is whether defendants needed a warrant to search his account. If they did, then they violated the Fourth Amendment because it's undisputed that defendants didn't have a warrant. If they didn't need a warrant, the question is whether the search had a reasonable purpose and scope.

But these substantive questions don't resolve defendants' motion for summary judgment. Even if defendants violated Bowers's Fourth Amendment rights, defendants contend that they are entitled to qualified immunity, a doctrine that shields public officials from damages under certain circumstances. Bowers isn't seeking injunctive relief, so if defendants prevail on their qualified immunity defense, his claim fails.

Generally, a defendant is entitled to qualified immunity unless the plaintiff shows not only that the defendant violated his rights, but also that his rights were clearly established at the relevant time. The plaintiff can meet this burden by pointing to either: (1) a closely analogous, binding case that was decided in his favor; (2) a more general constitutional rule that applies "with obvious clarity" to the defendants' conduct. *Cibulka v. City of Madison*, 992 F.3d 633, 639–40 (7th Cir. 2021). Defendants contend that Bowers has failed to meet his burden under either approach.

Defendants also invoke an aspect of qualified immunity doctrine that applies when the law is clearly established, but the defendant can show through "extraordinary circumstances" that he neither knew nor should have known of the relevant legal standard. *See Harlow v. Fitzgerald*, 457 U.S. 800, 818–19 (1982). Defendants contend that extraordinary circumstances are present in this case because they relied on the advice of counsel before deciding to conduct

the search. Following the advice of counsel might qualify as an extraordinary circumstance, and the court of appeals has considered factors such as whether the advice was unequivocal, whether it was specifically tailored to the particular facts giving rise to the controversy, and whether the attorney had all the relevant information. *Davis v. Zirkelbach*, 149 F.3d 614, 620 (7th Cir. 1998).

For reasons explained in the following sections, the court concludes that Bowers had a reasonable expectation of privacy in his Dropbox account and that defendants should have obtained a warrant before searching his account. But the court will grant defendants' motion for summary judgment because it was not clearly established that Bowers had a reasonable expectation of privacy or that any search by defendants fell outside the warrant exception for searches in the employment context. *See Shields v. Burge,* 874 F.2d 1201, 1206–07 (7th Cir. 1989) (plaintiff must show that it was clearly established that he had a reasonable expectation of privacy); *Gossmeyer v. McDonald*, 128 F.3d 481, 497 (7th Cir. 1997) (plaintiff must show that it was clearly established that warrant exception for employment-related searches doesn't apply). Although a search must be reasonable even in the absence of a warrant requirement, defendants' conduct meets that standard. Defendants are thus entitled to qualified immunity.

B. Bowers's expectation of privacy in his Dropbox account

To determine whether the government has conducted a "search" within the meaning of the Fourth Amendment, the Supreme Court has applied two tests. The first asks whether the government committed what would qualify as a trespass under common law. *United States v. Sweeney*, 821 F.3d 893, 899–900 (7th Cir. 2016). The second test asks whether the government intruded upon the plaintiff's reasonable expectation of privacy. *See United States v. Huart,* 735 F.3d 972, 974 75 (7th Cir. 2013) (plaintiff must show both that he had a subjective

expectation and that his expectation was objectively reasonable). In this case, both sides apply only the second test, so the court will follow that approach.

Whether an expectation of privacy is reasonable depends on context. *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (plurality opinion). The question for Bowers's claim isn't whether he had a general expectation of privacy in his Dropbox account, but whether he had a reasonable expectation of privacy specifically from intrusions by his employer. *See Mancusi v. DeForte*, 392 U.S. 364 (1968) (employee may have reasonable expectation of privacy from police, but not from a work supervisor).

The court begins with a review of the current state of the law. A difficulty for Bowers is that his claim arises out of the intersection of two areas of law that are largely unsettled: a government employee's expectation of privacy from his employer and an individual's expectation of privacy in electronic data. The Supreme Court has decided only a few cases on either issue.

O'Connor established that the Fourth Amendment applies to government employers, and the Court held that a public employee had a reasonable expectation of privacy in the contents of his office desk and file cabinets. 480 U.S. at 719.[3] But that holding was highly fact-specific, relying on several facts: the employee did not share his desk or file cabinets with any other employees; he had been the sole occupant of the office for 17 years; only the employee's personal documents were found inside the desk and cabinets; and the employer didn't have a policy that discouraged employees from storing personal items in their desks and

[3] There was no majority opinion in *O'Connor*, but the Court of Appeals for the Seventh Circuit has concluded that the plurality opinion is controlling. *Gustafson v. Adkins*, 803 F.3d 883, 892 (7th Cir. 2015). All citations to *O'Connor* are to the plurality opinion.

cabinets. *O'Connor*, 480 U.S. at 718–19. The Court expressly declined to articulate a clear, general rule for determining a government employee's reasonable expectation of privacy: "Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." 480 U.S. at 718.

City of Ontario v. Quon is the only other relevant case in which the Supreme Court considered an employee's reasonable expectation of privacy against the intrusions of a government employer. 560 U.S. 746 (2010).[4] The question was whether the city had violated the Fourth Amendment rights of a police officer by reviewing text messages that he had sent and received on a pager provided by the city. The Court considered several factors that could inform a determination whether the employee had a reasonable expectation of privacy in his text messages, including whether the city had given the employee notice that his text messages could be searched and the nature of the city's reasons for reviewing the messages. *Id.* at 758. But the Court declined to say whether the employee had a reasonable expectation, concluding that it was necessary to "proceed with care" because of the "difficulty predicting how employees' privacy expectations will be shaped by . . . changes [in technology] or the degree to which society will be prepared to recognize those expectations as reasonable." *Id.* As a result, the Court simply assumed that there was a reasonable expectation of privacy and resolved the case on other grounds. *Id.* at 760.

[4] The Supreme Court considered the appropriate standard for government employee drug testing in *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989), but neither side contends that *Von Raab* is instructive in this case.

The Court's cases regarding electronic privacy outside the workplace provide little additional guidance. The parties discuss two cases, *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United* States, 138 S. Ct. 2206, 2220 (2018). In *Riley*, the Court held that police can't search the contents of a cell phone under the doctrine that allows searches of some physical objects at the time a suspect is arrested. 573 U.S. at 386. The Court concluded that cell phones aren't comparable to most physical objects because cell phones contain "vast quantities of personal information" and allow the user to access even more personal information stored on the cloud. *Id.* at 386, 397.

In *Carpenter v. United States*, the Court considered whether cell phone users have a reasonable expectation of privacy in their location information even though such information can be accessed by the wireless carrier. Under the so-called third-party doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979), "even if the information is revealed on the assumption that it will be used only for a limited purpose," *United States v. Miller*, 425 U.S. 435, 443 (1976). The Court declined to extend *Smith* and *Miller* to cell phone location information, relying on two reasons: (1) cell phone location information is more revealing than the type of information at issue in *Smith* (telephone logs) and *Miller* (bank records); and (2) cell phone location "is not truly 'shared' as one normally understands the term" because carrying a cellphone "is indispensable to participation in modern society" and tracking occurs automatically, without an "affirmative act" by the user. *Carpenter*, 138 S. Ct. at 2220. But the Court also stressed that its decision was "a narrow one" and that the Court must "tread carefully" to "ensure that we do not embarrass the future." *Id. Riley* and *Carpenter* show that

the Court is concerned with protecting electronic privacy but also that the Court is proceeding cautiously and on a case-by-case basis rather than establishing bright-line rules.

Bowers also cites one precedential Seventh Circuit case, *Narducci v. Moore*, 572 F.3d 313 (7th Cir. 2009). In that case, the plaintiffs alleged that their public employer had been secretly recording all of their telephone calls. The court rejected the employer's qualified immunity defense, relying on both *O'Connor* and *Katz v. United States*, 389 U.S. 347, 353 (1967), which held in a nonemployment context that individuals using a telephone booth have a reasonable expectation of privacy in their conversations. The court also cited two other federal appellate opinions that reached the same conclusion. *Narducci*, 573 F.3d at 322.[5]

Against that legal backdrop, the court turns to the facts relied on by the parties to establishing or refute Bowers's reasonable expectation of privacy. The court begins with the county's IT policy, which is a cornerstone of both sides' arguments. That policy, which Bowers received and signed, provides:

> Taylor County retains exclusive ownership and control of all hardware, software, and the data that is generated through the use of its facilities. The Information Technology Department reserves the right to monitor all information technology usage and to access any electronic communications at any time. I have no expectation of privacy for any material on Taylor County equipment, even if that material was generated for my personal use.

[5] This court found three other Seventh Circuit cases addressing searches of government employees by their employers. *See Gustafson*, 803 F.3d at 892 (rejecting qualified immunity defense under Fourth Amendment on claim by female employee that employer was secretly conducting video surveillance of the changing room); *Gossmeyer*, 128 F.3d at 497 (upholding search of employee's office, desk, and cabinets); *Shields*, 874 F.2d at 1205–06 (upholding search of employee's desk). Neither side relies on these cases, and they provide little guidance, so the court won't discuss them further.

Dkt. 48, ¶ 5. Defendants contend that the policy forecloses any claim of a reasonable expectation of privacy, citing cases such as *Muick v. Glenayre Electronics,* which stated that an employee didn't have a reasonable expectation of privacy in his work computer because his employer had a policy of inspecting the laptops. 280 F.3d 741, 743 (7th Cir. 2002). "The laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to." Numerous other courts have reached a similar conclusion. *See also Rissetto v. Clinton Essex Warren Washington Bd. of Cooperative Educ. Servs*., No. 8:15-CV-720 (CFH), 2018 WL 3579862, at *6 (N.D.N.Y. July 25, 2018) ("[I]t appears that the majority of courts have accorded great weight to the existence of an employer's computer usage policy.").

But the court isn't persuaded that the county's IT policy actually applies to Bowers's Dropbox account. The policy states that employees have no expectation of privacy for material "on Taylor County equipment," but it's undisputed that Bowers's Dropbox account was stored on the cloud, not on county servers. Defendants also point to the language that the county may "access any electronic communications at any time." But Bowers's Dropbox account wasn't an electronic communication, so that provision doesn't apply either.

This leaves the IT policy provision that gives the county the right to "monitor all information technology usage." Defendants emphasize the word "all," contending that it extends beyond the county's own equipment. But that's not a reasonable interpretation, as it suggests that the county could monitor its employees on any personal electronic device anytime, anywhere, and for any purpose. The more reasonable interpretation is that the policy applies to technology use that is either done while on the job or on a county device. Defendants want to construe the provision broadly to include any technology use that is "work-related."

But the policy doesn't say that the county may access private accounts stored outside the county's computer system.

Both *O'Connor* and *Narducci* relied on the absence of an applicable policy to find a reasonable expectation of privacy, so that provides some support for Bowers's claim. But *O'Connor* and *Narducci* only go so far. The lack of an applicable policy was only one factor the courts considered. And *O'Connor* expressly stated that "the absence of . . . a policy does not create an expectation of privacy where it would not otherwise exist." 408 U.S. at 719. Furthermore, there was simply *no* policy addressing the general conduct at issue in those cases. Here, the policy cited by defendants does address electronic privacy, and it communicates an intent by the county to reserve its rights to monitor its employees' electronic data to the broadest extent possible. Certainly, Bowers was on notice that his electronic privacy was severely curtailed on work-related matters. So *O'Connor* and *Narducci* are distinguishable on this point. But the absence of a policy directly on point also distinguishes *Muick*, suggesting that it is necessary to consider other factors.

Bowers does points to other factors suggesting that the account was private and personal. He notes that he paid for the account, it was stored on the cloud rather than the county's computers or servers, and the account was password protected.

As a matter of common sense, these facts favor the conclusion that Bowers had a reasonable expectation of privacy. But there is surprisingly little case law in this circuit regarding an individual's reasonable expectation of privacy in an online account. Bowers cites *Antonelli v. Sherrow* for the proposition that passwords create a reasonable expectation of privacy. 246 F. App'x 381, 384 (7th Cir. 2007). But that case isn't precedential, and it simply observed that the Court of Appeals for the Fourth Circuit had reached that conclusion in the

context of a password-protected computer. The actual holding in *Antonelli* was that the plaintiff didn't have an expectation of privacy because he shared his password with his ex-wife. *Id.*

Since *Antonelli*, other courts have held that password protections can create a reasonable expectation of privacy. *See United States v. Thomas*, 818 F.3d 1230, 1241–42 (11th Cir. 2016); *United States v. Heckenkamp,* 482 F.3d 1142, 1146–47 (9th Cir. 2007); *United States v. Andrus,* 483 F.3d 711, 719 (10th Cir. 2007). Defendants don't cite any contrary authority. "[A] robust consensus of cases of persuasive authority" can be sufficient to overcome a qualified immunity defense. *Est. of Davis v. Ortiz*, 987 F.3d 635, 638 (7th Cir. 2021). And these cases are consistent with the well-established rule that individuals generally have a reasonable expectation of privacy in locked or closed containers, which are comparable to a password-protected account. *See United States v. Basinski,* 226 F.3d 829, 835 (7th Cir. 2000); *United States v. Neff,* 61 F.3d 906 (7th Cir. 1995). So if the question were simply whether it was clearly established that an employee has a reasonable expectation of privacy in a password-protected, private, online account, the answer would likely be yes.

But defendants rely on several other factors to support the conclusion that Bowers didn't have a reasonable expectation of privacy, including the following:

1) Bowers used his work email address to create and access the account;

2) he used his work computer to copy the files at issue to his Dropbox account;

3) he gave multiple crew members and his girlfriend access to his Dropbox account;

4) Dropbox's privacy policy allowed the company to review and share the contents of his account under certain circumstances;

5) he believed that he was acting within the scope of his employment when he transferred the files; and

6) the contents of the account included work-related files.[6]

To sum up, the thrust of defendants' argument goes something like this: if Bowers didn't want defendants to access his account, he shouldn't have connected the account to his work email and put files from a work computer on that account, and then shared access to the account with multiple parties. According to defendants, that conduct is inconsistent with both a subjective expectation of privacy and a reasonable one.

The facts cited by defendants do show that there was a connection between Bowers's account and his employer and that any expectation of privacy was diminished by Bowers's own conduct. And it makes some sense to say that the county should have had at least as much access to its own files than third parties affiliated with a television show who weren't supposed to see those files without county authorization. But the court concludes that Bowers retained a reasonable expectation of privacy despite these other facts.

As already noted, Bowers did take some steps to keep the account private from defendants. Linking the account to his work email blurs the boundary between his work and private spaces, but the county's IT policy says nothing about monitoring private accounts that are linked to work email. In the absence of a clearer notice from the county, Bowers was entitled to assume that a private account was private. *Cf. Narducci*, 572 F.3d 313.

As for sharing the account with the TV crew members and a friend, that doesn't mean that Bowers was inviting anyone to view his account. By way of comparison, homeowners don't

[6] In their reply brief, defendants argue for the first time that police officers have a reduced expectation of privacy compared to other public employees. Dkt. 49, at 12–14. Defendants forfeited that argument by failing to raise it in their opening brief. *See White v. United States*, 8 F.4th 547, 552–53 (7th Cir. 2021).

forfeit a reasonable expectation of privacy against intrusions by the police if they invite friends to stay with them.

The court reaches the same conclusion regarding Dropbox's privacy policy, which gave Dropbox the right to "access, store, and scan" Bowers's information, as well as to disclose it to third parties for various reasons, including to comply with the law. Dkt. 31-2, at 1, 7. The right of a commercial entity to gain access to an account doesn't mean the government has the same right.

At first blush, this conclusion may seem to be in tension with the so-called third-party doctrine discussed above, under which a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 443. But the third-party doctrine doesn't necessarily apply to this case. *Smith* and *Miller* are about an expectation of privacy in particular *information*; the question in both cases was whether the government needed a warrant before seeking information from a third party who also has access.

In this case, Bowers isn't contending that he had a right to keep the case files themselves private. Bowers's claim is about restricting *access* to his account, not protecting the particular files at issue or preventing third parties from sharing the files. One can lose a right to keep information private by disclosing it to the public, but that doesn't mean the government can force entry into someone's home on the ground that the home contains public documents. As another example, if someone sends an email to a friend, the Fourth Amendment won't prevent the friend from sharing the contents of the email with the police, but that doesn't mean the police are entitled to hack an email account because all the emails are being shared with a third party. *See United States v. Maxwell,* 45 M.J. 406, 417–19 (C.A.A.F. 1996).

Many cases involving the third-party doctrine involve information that the government actually received from the third-party. For example, courts have consistently held that the government doesn't intrude on a reasonable expectation of privacy by obtaining information from a nonpublic Facebook account if that information was shared by one of the user's "friends." *Palmieri v. United States*, 72 F. Supp. 3d 191, 209 (D.D.C. 2014), *aff'd*, 896 F.3d 579 (D.C. Cir. 2018). In this case, defendants didn't obtain access to Bowers's account through the Dropbox company or through one of the third parties who had access to the account, so those cases are distinguishable.

Bowers analogizes his situation to that of a hotel guest, who has a reasonable expectation of privacy even though hotel staff have access to the room. *See Stoner v. California*, 376 U.S. 483, 489–90 (1964). Bowers also cites *United States v. DiTomasso*, in which the court concluded that monitoring of email communications for commercial purposes doesn't waive the sender's expectation of privacy. 56 F. Supp. 3d 584, 591 (S.D.N.Y. 2014). The court reasoned that use of electronic devices is necessary for "meaningful participation in social and professional life," and that such use "almost always requires acquiescence to some manner of consent-to-search terms," so applying a waiver principle in those circumstances would lead to the "evisceration of the Fourth Amendment." *Id.* at 592. Both the reasoning of *DiTammasso* and the analogy to *Stoner* are persuasive.

The problem for Bowers is that neither a district court case nor a Supreme Court case about a significantly different issue would have made it clear to defendants that their conduct was unlawful under the circumstances of this case. Although Bowers contends that cases such as *Katz*, *O'Connor*, and *Riley* made it obvious that he had a reasonable expectation of privacy, those cases establish only general principles. And the Supreme Court has "repeatedly told

courts not to define clearly established law at too high a level of generality." *City of Tahlequah, Oklahoma v. Bond*, 142 S. Ct. 9, 11 (2021).

The uncertainty in the law is shown by the cases that defendants cite. For example, in *Clark v. Teamsters Local Union 651*, an employer used the "lost password" feature to search for work-related files stored in a Dropbox account of an employee who used his work email to set up the account. 349 F. Supp. 3d 605, 621 (E.D. Ky. 2018). The court concluded that the employer didn't violate the employee's rights, reasoning as follows:

> While not explicitly addressed by the Sixth Circuit, district courts have held an employee does not have a reasonable expectation of privacy in e-mails sent or received using a work e-mail address. *See Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 WL 974676 at *2, 2002 U.S. Dist. LEXIS 8343 at *5 (D. Mass. 2002) (explaining even in the absence of a company e-mail policy, employees did not have a reasonable expectation of privacy in their work e-mail); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (holding no reasonable expectation of privacy in voluntary e-mail communications made by an employee, notwithstanding any assurance that e-mails would not be intercepted by management). If individuals do not have a reasonable expectation of privacy in their work e-mails, then it logically follows that individuals do not have a reasonable expectation of privacy in a Dropbox account that is tied to their work e-mail and that they lose access to if they lose access to the e-mail.

Id. As Bowers is quick to point out, *Clark* involved a claim for intrusion upon seclusion rather than a violation of the Fourth Amendment. But both types of claims consider an employee's reasonable expectation of privacy, so it is instructive on whether the law would be clearly established to an employer considering a search.

In its own research, the court found *Frankhouser v. Clearfield County Career & Technical Center*, a Fourth Amendment case in which a government employer accessed an employee's password-protected Dropbox account, which included both work-related and personal information. No. 3:18-CV-180, 2019 WL 1259570, at *1–2 (W.D. Pa. Mar. 19, 2019). In

denying the defendant's motion to dismiss, the court observed that the case "does not fit easily within Fourth Amendment precedent," that the Supreme Court has directed courts to "'[p]roceed with care' when considering privacy expectations in the context of modern technology," that there is a "paucity of case law discussing Dropbox and privacy expectations," and that the case was only at the pleading stage. *Id.* at *7. *Frankhauser* provides some substantive support for Bowers's claim, but it also underscores the uncertainty in this area of the law. Notably, the defendants in *Frankhauser* didn't assert a qualified immunity defense.

As for Bowers sharing access to his account, defendants cite *United States v. Maclin*, in which the court held that the defendant didn't have a reasonable expectation of privacy in a password-protected Dropbox account because the account was shared with others. 393 F. Supp. 3d 701, 711 (N.D. Ohio 2019). Similarly, other courts have held that there is no reasonable expectation of privacy in a computer network when the network is shared, even if it is a closed network that is shared with "friends" only. *United States v. Giboney*, No. 4:15CR97JAR (SPM), 2016 WL 873325, at *7 (E.D. Mo. Feb. 18, 2016) (collecting cases). These cases do not clearly explain why even selectively shared access with an account or a network completely destroys an expectation of privacy, which limits the cases' persuasiveness. And Bowers points out that *Maclin* is distinguishable because that case involved a shared password, whereas Bowers shared access without sharing his password.

But whatever the limitations of defendants' authority, Bowers cannot prevail by showing that defendants have failed to disprove his claim. It is his burden to show that the law was clearly established. And the bottom line is that Bowers hasn't cited Supreme Court or Seventh Circuit law clearly establishing that he retained a reasonable expectation of privacy against intrusions by the county despite his linking the account to his work email, putting

confidential work files from a work computer in the account, and sharing access to the account with others. The precedential authority he relies on provide the general principles that provide the foundation for his claim. But that case law doesn't show that the contours of the law were so well defined that it would be clear to a reasonable officer in defendants' position that Bowers had a reasonable expectation in keeping his Dropbox account private from the county. *See Bond*, 142 S. Ct. at 11. In the absence of such a showing, defendants are entitled to summary judgment on the basis of qualified immunity.

C. Reasonableness of the search of Bowers's Dropbox account

Even if Bowers had a clearly established reasonable expectation of privacy in his Dropbox account, his claim would still fail. A reasonable expectation of privacy means only that defendants conducted a search within the meaning of the Fourth Amendment. The next question is whether that search was unreasonable. The general rule is that searches conducted without a warrant are per se unreasonable. *Riley*, 573 U.S. at 401. It is undisputed that defendants didn't have a warrant for their search, but there are several exceptions to the warrant requirement, and defendants contend that one of those exceptions applies here.

To determine the reasonableness of the search, the court must first consider whether an exception to the warrant requirement applies. If it doesn't, the search was unreasonable. But if an exception does apply, the question is the whether the search was a reasonable application of the exception. The court concludes that: (1) defendants should have obtained a warrant, but the law wasn't clearly established on that point; and (2) the search was a reasonable application of the government-employer exception to the warrant requirement. So defendants are entitled to summary judgment on the issue of reasonableness as well.

1. Warrant requirement

One of the exceptions to the warrant requirement applies to certain searches by government employers. "[W]ork-related searches are merely incident to the primary business of the agency. Under these circumstances, the imposition of a warrant requirement would conflict with the common-sense realization that government offices could not function if every employment decision became a constitutional matter." *O'Connor*, 480 U.S. at 721–22.

The parties dispute the scope of the exception, and they dispute whether the exception applies here. Bowers contends that the exception applies only to areas that are within the employer's control. Defendants' position is that the exception applies so long as the purpose of the government employer's search was "work-related."[7]

Defendants' position is understandable because *O'Connor* repeatedly uses the phrase "work-related" when discussing the government-employer warrant exception. *E.g.,* 480 U.S. at 722 ("[W]ork-related searches are merely incident to the primary business of the agency."); *id.* at 724 ("We come to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct."). And in one provision, the Court appears to be announcing a standard, using the concept of "work-related" as a defining feature: "We hold, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for

[7] Bowers doesn't contend that a warrant was required because he was later criminally charged for the same conduct that defendants were investigating, so the court need not consider that issue. *Compare Driebel v. City of Milwaukee,* 298 F.3d 622, 639–40 (7th Cir. 2002) (concluding that *O'Connor* didn't apply to searches of policemen who "were advised at one time or another that they were criminal suspects who were questioned with an eye towards criminal prosecution") *with United States v. Fernandes*, 272 F.3d 938, 943 n.3 (7th Cir. 2001) (*O'Connor* applied to search of deputy prosecutor's office because the prosecutor who ordered the search "was not conducting a criminal investigation" at the time he ordered the search).

investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances." *Id.* at 725.

But a closer look at the opinion reveals that the Court is using "work-related" as shorthand for a more nuanced standard. At the beginning of the opinion, the Court sets forth the scope of its rule: "Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. *The workplace includes those areas and items that are related to work and are generally within the employer's control*." 480 U.S. at 715–16 (emphasis added).

The Court goes on to say in the next paragraph that "[n]ot everything that passes through the confines of the business address can be considered part of the workplace context" and that "[t]he appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address." *Id.* at 716. Thus, in describing the "workplace context," the Court was defining the contours of the government-employer warrant exception. There would have been no reason for the Court to suggest that personal items such as closed luggage may be governed by a different standard if the employer's purpose was all that mattered. *See James v. Hampton,* 592 F. App'x 449, 457 (6th Cir. 2015) (concluding that *O'Connor* didn't apply to search of personal safe that employee kept in her office). In later portions of the opinion, it wasn't necessary for the Court to be more precise because the case at hand involved a search of a government office and government property.

Moreover, under defendants' view, government employers could force entry into an employee's home without a warrant so long as their reason for doing so was work-related.

Defendants cite no authority for that view, and several courts have held that a government employer must obtain a warrant or qualify for another exception under those circumstances. *See*, *e.g.*, *Lesher v. Reed*, 12 F.3d 148, 150–51 (8th Cir. 1994); *Los Angeles Police Protective League v. Gates*, 907 F.2d 879, 886 (9th Cir. 1990); *Sabin v. Miller*, 423 F. Supp. 2d 943, 949–51 (S.D. Iowa 2006). For these reasons, the court concludes that *O'Connor* doesn't apply, and that defendants should have obtained a warrant because Bowers stored the files at issue in a private, online account rather than in an area "generally within the employer's control."

That being said, *O'Connor* didn't explain what it means for an area to be "generally within the employer's control." In a sense, the Dropbox account was within defendants' control because of Bowers's decision to link the account to his work email. Again, that's the reason that defendants were able to access Bowers's account in the first place.

Also creating ambiguity are the reasons provided in *O'Connor* for dispensing with the warrant requirement. The Court stated that "public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner," "the consequences of [employee] misconduct or incompetence to both the agency and the public interest can be severe," and imposing a warrant requirement "would seriously disrupt the routine conduct of business and would be unduly burdensome." *O'Connor*, 408 U.S. at 722, 724. Whether Bowers stored the stolen files on a work computer or in a private, online account, the effect on the department and the public interest was the same.

Neither side cites any cases in which the Supreme Court or any other court has provided further guidance. As noted above, this court has found cases holding that *O'Connor* doesn't apply to the search of an employee's home, but a home is unequivocally outside the employer's control and also at the core of the Fourth Amendment's protections. *See Caniglia v. Strom*, 141

S. Ct. 1596, 1599 (2021). A shared, online account connected to a work email address isn't obviously encompassed by case law about a person's private residence.

In the absence of clear authority holding that *O'Connor* does not apply to the facts of this case, Bowers cannot show that defendants violated his clearly established rights by failing to get a warrant before searching his Dropbox account.

2. Reasonableness of the search under *O'Connor*

Even when a warrant isn't required, a search must still be reasonable. In the public employment context, courts consider both the initial decision to conduct a search and the scope of the search. *O'Connor*, 480 U.S. at 725–26. The initial decision is reasonable when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct; the scope is reasonable if it is reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct. *Id.*

That standard is satisfied in this case. At the time defendants conducted the search, Bowers had already admitted that he had shared files with crew members, Woebbeking had overheard crew members talking about receiving documents on Dropbox, and a county employee who had been retrieving paper files for Bowers told Woebekking that she believed case files had been released to Dropbox. This information provided defendants with reasonable grounds to believe that they would find evidence of work-related misconduct in Bowers's Dropbox account.

The scope of the search was also reasonable. Defendants accessed the account to locate county files and to find out with whom Bowers shared those files. Bowers doesn't allege that defendants viewed or copied any of his personal files.[8]

Bowers says that the search was unreasonable in scope for three reasons: (1) the county's IT policy didn't authorize defendants' conduct; (2) Bowers protected the account with a password and stored personal files in the account; and (3) Bowers had been "cooperative" with Daniels up until that point. Dkt. 46, at 25. The first two reasons are related to the reasons Bowers believes that he had a reasonable expectation of privacy in his account, and the court need not consider those issues again.

Bowers doesn't elaborate on the third reason, but presumably he means that he would have voluntarily returned or deleted any electronic files if defendants had asked him to do so. But the Supreme Court has already rejected a nearly identical argument. In *Quon*, the police officer argued that his employer's search of his text messages was unreasonable in part because the employer could have asked him for permission to review his text messages. 560 U.S. at 763. The Court concluded that the argument "was inconsistent with controlling precedents" because the Court had "repeatedly refused to declare that only the least intrusive search practicable can be reasonable under the Fourth Amendment." *Id.*

The same conclusion applies here. Perhaps Bowers would have fully disclosed on his own all the files he shared and with whom he shared them. Or perhaps not. It's undisputed that Bowers attempted to delete all the case files in the account after defendants first accessed

[8] Defendants accessed Bowers's account a second time "to shut off all access to the Dropbox from any remote device." Dkt. 48, ¶ 115. But Bowers doesn't challenge that conduct, so the court won't consider it.

it. Dkt. 48, ¶ 110. Regardless, defendants weren't required under the law to give Bowers the benefit of the doubt.

D. Conclusion

The court concludes that defendants violated Bowers's Fourth Amendment rights by failing to get a warrant before searching his Dropbox account. But the law didn't clearly establish that defendants needed a warrant under the circumstances of the case, and defendants' search of the account was otherwise reasonable. So defendants are entitled to qualified immunity, and the court will grant their motion for summary judgment.

ORDER

IT IS ORDERED that the motion for summary judgment filed by defendants Bruce Daniels, Melissa Seavers, and Taylor County, Dkt. 28, is GRANTED. The clerk of court is directed to enter judgment in defendants' favor and close this case.

Entered April 14, 2022.

BY THE COURT:

/s/

_____

JAMES D. PETERSON
District Judge